	Application No.	Applicant(s)
Notice of Allowability	10/057,255	HAMADA, MASASHI
	Examiner	Art Unit	
	·Ranodhi Serrao	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. THIS · NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS. This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *15 May 2007*.

2. ☒ The allowed claim(s) is/are *1,5-10,12-15,17-19,22-24,26-35,38,61 and 84*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some*   c) ☐ None of the:

       1. ☒ Certified copies of the priority documents have been received. ʼ

       2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

       3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the

         International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

      Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

1.   An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be

submitted no later than the payment of the issue fee.

2.   Authorization for this examiner's amendment was given in a telephone interview

with Ping Gu (Reg. No. L0040) on 30 May 2007.

ALLOWABLE CLAIMS

This listing of claims will replace all prior listings of claims in the application.

Listing Of Claims:

Claim 1 (currently amended):   A data management method using a

network system which includes a server, a client terminal and a plurality of data servers,

comprising:

a reception step of making the server receive a user's data storage

request and data to be stored from the client terminal;

a select step of making the server automatically select data servers for

storing the data from the plurality of data servers, the selected data servers being

different from each other and including at least a first data server and a second data

server, said first data server being located in an area which is different from an area of

user's address registered by the user of the client terminal, said second data server

being located in an area with a disaster rate of occurrence equal to or smaller than a

predetermined threshold; ~~and~~

a storage step of making the server send the data to the selected data

servers, and store the data in the selected data servers[.]; and

a step of making the server acquire disaster information from a disaster

information database that provides disaster information, and search for the area with

said disaster rate of occurrence equal to or smaller than said predetermined threshold

on the basis of the acquired disaster information for selecting the server in the select

step.

Claim 2-3 (canceled)

Claim 4 (canceled)

Claim 5 (previously presented): The method according to claim 1,

further comprising:

a step of making the server encrypt the data, and

wherein the storage step includes the step of:

making the server send the data encrypted by different methods to the

respective data servers, and store the data in the data servers.

Claim 6 (previously presented): The method according to claim 5,

further comprising:

a step of making the server periodically acquire the encrypted

data from the data servers;

a step of making the server decrypt the acquired data; and

a step of making the server compare the decrypted data.

Claim 7 (previously presented): The method according to

claim 1, further comprising:

a step of making the server send to the client terminal addresses of the

data servers that store the data.

Claim 8 (previously presented): The method according to claim 5,

further comprising:

a step of making the server send to the client terminal addresses of the

data servers that store the data, and a key used to decrypt the encrypted data.

Claim 9 (previously presented): The method according to claim 1,

wherein information of the user's address is pre-stored in the server.

Claim 10 (previously presented):   The method according to claim 1,

further comprising:

a step of making the data server receive a user's data transmission

request from the client terminal; and

a step of making the data server send data associated with the data

transmission request to the client terminal.

Claim 11 (canceled)

Claim 12 (currently amended): A server comprising:

reception means for receiving a user's data storage request and data to be stored sent from a client terminal;

select means for automatically selecting data servers for storing the data from a plurality of data servers, the selected data servers being different from each other and including at least a first data server and a second data server, said first data server being located in an area which is different from an area of user's address registered by the user of the client terminal, said second data server being located in an area with a disaster rate of occurrence equal to or smaller than a predetermined threshold; and

sending means for sending the data to the selected data servers via a communication line[.]; and

searching means for acquiring disaster information from a disaster information database that provides disaster information, and searching for the area with said disaster rate of occurrence equal to or smaller than said predetermined threshold on the basis of the acquired disaster information for selecting the server by the select means.

Claim 13 (currently amended): A computer program [for] making a computer function as:

reception means for receiving a user's data storage request and data to be stored sent from a client terminal;

select means for automatically selecting data servers for storing

the data from a plurality of data servers, the selected data servers being different

from each other and including at least a first and a second data server, said first

data server being located in an area which is different from an area of user's

address registered by the user of the client terminal, said second data server

being located in an area with a disaster rate of occurrence equal to or smaller

than a predetermined threshold;~~and~~

sending means for sending the data to the selected data servers via a

communication line[.]; and

searching means for acquiring disaster information from a disaster

information database that provides disaster information, and searching for the area with

said disaster rate of occurrence equal to or smaller than said predetermined threshold

on the basis of the acquired disaster information for selecting the server by the select

means.

Claim 14 (currently amended): A data management system including a

control server, a client terminal, and a plurality of data servers, which can communicate

with each other via a communication line,

said control server comprising:

reception means for receiving a user's data storage request and

data to be stored sent from the client terminal;

select means for automatically selecting data servers for storing

the data from the plurality of data servers, the selected data servers being

different from each other and including at least a first data server and a second

data server, said first data server being located in an area which is different

from an area of user's address registered by the user of the client terminal, said

second data server being located in an area with a disaster rate of occurrence

equal to or smaller than a predetermined threshold;~~and~~

   sending means for sending the data to the selected data servers[.]; and

   searching means for acquiring disaster information from a disaster

information database that provides disaster information, and searching for the

area with said disaster rate of occurrence equal to or smaller than said

predetermined threshold on the basis of the acquired disaster information for

selecting the server by the select means; and

   said data servers comprising:

   means for storing the data sent from said control server.

Claim 15 (previously presented): The server according to claim 12,

wherein said select means automatically selects the data server based on the user's

service subscription qualification level.

Claim 16 (canceled)

Claim 17 (previously presented): The server according to claim 15

wherein said sending means encrypts the data using an encryption method

corresponding to the data servers selected by said select means.

Claim 18 (previously presented): The server according to claim 15, wherein the service subscription qualification level is determined based on a subscription fee for a service.

Claim 19 (previously presented): The server according to claim 15, wherein the service subscription qualification level is determined based on a service subscription term.

Claim 20-21 (canceled)

Claim 22 (previously presented): The server according to claim 15, wherein said select means selects a data server with a lowest suffering risk from the plurality of data servers corresponding to the service subscription qualification level of the user who issued the storage request, and a server with a lowest suffering risk of the data servers in a different area from the area of user's address registered by the user who issued the storage request.

Claim 23 (previously presented): The server according to claim 15, wherein when the user's service subscription qualification level has changed, said select means re-selects the data servers, and said sending means sends the data again to the data servers re-selected by said select means.

Claim 24 (previously presented): The server according to claim 15, wherein said select means re-selects the data servers in accordance with a change in

disaster information, and said sending means sends the data again to the data servers

re-selected by said select means.

Claim 25 (canceled).

Claim 26 (previously presented): The server according to claim 15,

further comprising checking means for checking authenticity of the data stored in the

data server.

Claim 27 (previously presented): The server according to claim 26,

wherein said checking means checks authenticity by comparing data which are

associated with an identical storage request and are stored in the data servers.

Claim 28 (previously presented): The server according to claim 26,

wherein said checking means checks if data becomes fraudulent due to a memory

medium.

Claim 29 (previously presented): The server according to claim 26,

wherein said checking means checks if data becomes fraudulent due to tampering of

data.

Claim 30 (previously presented): The server according to claim 29,

wherein when said checking means determines that the data becomes fraudulent due to

tampering of data, said checking means sends a message indicating this to a client

terminal that issued the storage request of the data.

Claim 31 (previously presented): The server according to claim 15, further comprising authentication means for authenticating if the user who issued the storage request is a member who subscribes to the service, and accepts only the storage request from the user authenticated by said authentication means.

Claim 32 (previously presented): The server according to claim 15, further comprising authentication means for checking authenticity of the data server selected by said select means, and said sending means sends data in only the data servers authenticated by said authentication means.

Claim 33 (previously presented): The server according to claim 15, further comprising notify means for sending at least various storage condition data associated with a data storage process to a client terminal that issued the storage request.

Claim 34 (previously presented): The server according to claim 33, wherein said notify means sends encryption algorithm and key data in addition to storage location data of the data associated with the storage request as the storage condition data.

Claim 35 (previously presented): The server according to claim 33, wherein the client device includes storage means for storing at least the storage condition data sent from said notify means.

Claim 36-37 (canceled)

Claim 38 (previously presented): The method according to claim 1,

wherein the server automatically selects the data servers based on the user's service

subscription qualification level in the select step.

Claim 39-60 (canceled)

Claim 61 (previously presented): The system according to claim 14,

wherein said select means automatically selects the data servers based on the user's

service subscription qualification level.

Claim 62-83 (canceled)

Claim 84 (previously presented): The computer program according to

claim 13, wherein said select means automatically selects the data servers based on

the user's service subscription qualification level.

Allowable Subject Matter

3.   Claims 1, 5-10, 12-15, 17-19, 22-24, 26-35, 38, 61, and 84 are allowed. The

following is an examiner's statement of reasons for allowance: In interpreting the claims,

in light of the specification and the applicant's amendments filed on 30 May 2007, the

Examiner finds the claimed invention to be patentably distinct from the prior art of

record.

4.   **Petersen (2002/0103907)**, teaches utilizing the unused portions of storage

capacity on servers. Existing servers (e.g. vendor servers) are used to store data for

backup purposes. Data stored therein is preferably dispersed amongst multiple servers,

or can be limited to one server. When a customer requests storage space for backup of

data, a central server monitoring the servers tied into the service will check the

availability of storage space on the servers. The data will then be allocated to empty

space in the various servers, selected according to, for example, bandwidth of

transmission, availability, etc. **(Petersen, Abstract, Figure 1a, and corresponding**

text).

5.   **Staheli et al. (5,537,533),** teaches a system for remote mirroring of digital data

from a primary network server to a remote network server includes a primary data

transfer unit and a remote data transfer unit which are connectable with one another by

a conventional communication link. The primary data transfer unit sends mirrored data

from the primary network server over the link to the remote data transfer unit which is

located a safe distance away. Each data transfer unit includes a server interface and a

link interface. The server interface is viewed by the network operating system as

another disk drive controller. The link interface includes four interconnected parallel

processors which perform read and write processes in parallel. The link interface also

includes a channel service unit which may be tailored to commercial communications

links such as T1, E1, or analog telephone lines connected by modems **(Staheli,**

Abstract, Figure 2, and corresponding text).

6.   However, the prior art of record fails to teach or suggest individually or in

combination that A data management method using a network system which includes a

server, a client terminal and a plurality of data servers, comprising: a reception step of

making the server receive a user's data storage request and data to be stored from the client terminal; a select step of making the server automatically select data servers for storing the data from the plurality of data servers, the selected data servers being different from each other and including at least a first data server and a second data server, said first data server being located in an area which is different from an area of user's address registered by the user of the client terminal, said second data server being located in an area with a disaster rate of occurrence equal to or smaller than a predetermined threshold; a storage step of making the server send the data to the selected data servers, and store the data in the selected data servers; and a step of making the server acquire disaster information from a disaster information database that provides disaster information, and **search for the area with said disaster rate of occurrence equal to or smaller than said predetermined threshold on the basis of the acquired disaster information for selecting the server in the select step** as set forth in independent claims 1 and 12-14. Claims 1, 5-10, 12-15, 17-19, 22-24, 26-35, 38, 61, and 84 are allowed because of the combination of other limitations and the limitations listed above.

7.   Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ranodhi Serrao whose telephone number is (571) 272-7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RNS

R.N.S.

6/06/2007

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER